Katya Bespartochna
March 24th, 2020

Bring Your Own Device(BYOD) is a somewhat new and evolving trend where companies are letting employees bring in their own mobile devices to work to do employee-related activities. Many companies are finding that there are more benefits than drawbacks when employing the practices of this BYOD. At the same time, introducing BYOD into a company can resemble a certain type of anarchy in the information systems world. Employees are trying to figure out ways to control and be vulnerable to potential security breaches that come with the new policy.

The idea of BringYour Own Device came collectively from new end-users and their demands in the business worlds. Many Apple iOS and Android users did not want to carry two different devices and often asked the IT department the question of whether or not they can bring their own device to work.

One article studies a group of first-year college students. These students were divided into groups of four and five and were given case studies from a variety of different accounting firms. The students analyzed what would be world problems within the firms through a variety of different presentations. At the end of the simulation, students took a survey evaluating what they learned from Bring-your-Own-Device in the study. Most of the students agreed that implementing Bring Your Own Devices policies brought in more awareness of how the It world works and enhanced their experience.

There are several benefits that come with BYOD. Most of them come from the type of employees companies are now hiring. As the article *A bring-your-own-devices case for use in the classroom* mentions “Young adults aged 18-29 are especially likely to be ‘smartphone

dependant' and have deeply embedded devices into the daily contours of their life". When an employee brings their own device to work, they create instant and wider connections to employees without the need for the internet. This leads to fostering innovation and creativity. There is also a general increase in employee satisfaction. On the employers side, companies are able to retain tech-savvy employees. Cost is also reduced in areas like procurement, hardware, software, licensing, and insurance. People working in It benefit from collaboration and sharing which leads to enterprise growth(Sipior).

While the benefits of BYOD sound exciting, there are obvious drawbacks. One of them is that devices that people personally own can easily be stolen. Bring Your Own Device Survival Guide writes "McAfee, the security company, says that over 4 percent of smartphones are lost or stolen each year". This is the equivalent of one person out twenty-five people easily losing their phone without any contributing factors in the IT world. Another issue that relates to wi-fi. There is a growing number of hotspots that are made and opens regular activities done in companies to more vulnerability.

Trust is also an important aspect of BYOD. Security deals with large amounts of data and having BYOD in place blurs the line between personal entertainment and business related content. The type of encryption used in data becomes more trickier and confusing(Keyes).

There are a few sets of protection set in place to prevent the possibility of a phone or tablet getting stolen. Mobile devices need to have a Passcode that preferably erases its data after several failed attempts. It also needs a Remote lock which would disable all features except emergency and incoming calls. If the situation calls for it, the devices will need to have Remote wipe with remote erase capability(Gatewood).

To control some of these drawbacks, there are a few considerations one must have when managing BYOD like compatibility, compliance, and culture. Compatibility deals with the set of specifications that employee devices should meet. It is important to note that compatibility should be balanced with freedom, control and security. The compliance factors in BYOD considers and identifies legal and regulatory issues through a steering committee. The amount that employee is willing to comply with the Information Security structure policy, the more beneficial it is to the freedom aspect.

Keyes, Jessica. Bring your own devices (BYOD) survival guide. CRC press, 2013.

Sipior, Janice C., et al. "**A Bring-Your-Own-Device Case for Use in the Classroom.**" Communications of the Association for Information Systems, vol. 41, July 2017, pp. 216–241. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=bsu&AN=124670671&site=eds-live.

Gatewood, Brent. "The nuts and bolts of making BYOD work." Information Management Journal, vol. 46, no. 6, Nov.-Dec. 2012, p. 26+. Gale Academic OneFile, https://link.gale.com/apps/doc/A321579853/AONE?u=philbibu&sid=AONE&xid=777ffb37. Accessed 23 Mar. 2020.